

ON THE RANK OF CONGRUENT ELLIPTIC CURVES

FARZALI IZADI AND HAMID REZA ABDOLMALEKI

ABSTRACT. In this paper, p and q are two different odd primes. First, We construct the congruent elliptic curves corresponding to p , $2p$, pq , and $2pq$, then, in the cases of congruent numbers, we determine the rank of the corresponding congruent elliptic curves.

1. INTRODUCTION

The rank of an elliptic curve is a measure of the size of the set of rational points. However, the question is to ask how one can compute the exact size of this set of rational points. On the other hand, it is easy to find the rational points of a projective line or a plane curve defined by a quadratic equation. Having said that, there is no known guaranteed algorithm to determine the rank and it is not known which numbers can occur as the rank of an elliptic curve. (see [5]).

The rational number n is a congruent number if there are positive rational numbers a, b, c such that $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$, equivalently, there is a Pythagorean triangle with rational sides and the area equals to n .

In a modern language, n is a congruent number if and only if the elliptic curve $E : y^2 = x^3 - n^2x$ contains a rational point with $y \neq 0$, equivalently, a rational point of infinite order, i.e., the rank of E which is denoted by $r(E)$ is nonzero, (see [9]).

First we quote from Monsky [4]. Let p_1, p_3, p_5 and p_7 denote primes $\equiv 1, 3, 5$ and $7 \pmod{8}$. Heegner [3], and Brich [1], proved that $2p_3$ and $2p_7$ are congruent numbers. Heegner asserted without proof that p_5 and p_7 are congruent numbers, and this claim is repeated in [7]. Monsky [4] has given a unified proof that the following are all congruent numbers :

- (1) : $p_5, p_7, 2p_7$, and $2p_3$,
- (2) : $p_3p_5, p_3p_7, 2p_3p_5$ and $2p_5p_7$,
- (3) : p_1p_5 provided $(\frac{p_1}{p_5}) = -1$, and $2p_1p_3$ provided $(\frac{p_1}{p_3}) = -1$ and $p_1p_7, 2p_1p_7$, provided $(\frac{p_1}{p_7}) = -1$,

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 14H52, 14G05,
Key words and phrases. Elliptic curves, Rank, congruent numbers.

In other words, any $N = 5, 6$ or $7 \pmod{8}$ having at most 2 odd prime factors is a congruent number, with the following possible exception $N = pq$ or $2pq$ with $p \equiv 1 \pmod{8}$ and $(\frac{p}{q}) = +1$.

Remark 1.1. For N in the form of (1), (2) and (3), our proof shows that the rank of $E_N^{\mathbb{Q}} : Y^2 = X^3 - N^2X$ is 1. However, for $N = pq$ or $2pq$ with $p \equiv 1 \pmod{8}$ and $(\frac{p}{q}) = +1$, this result is not true. For example, for $N = (521).(5)$, the rank of $E_N^{\mathbb{Q}}$ is 3.

In section two, we recall the 2-descent method which is a classical method for finding the rank of elliptic curves. Section three includes our results and contains five parts.

In part (1), Let $E : y^2 = x^3 - p^2x$, be the corresponding congruent number elliptic curve for p . It is known that if $p \equiv 5, 7 \pmod{8}$ then p is congruent number (see[4]). Using the 2-descent method, we show in this two cases, $r(E) = 1$. Moreover if $p \equiv 3 \pmod{8}$ then $r(E) = 0$, i.e., p is not congruent.

In part (2), for $p \equiv 1 \pmod{8}$, we investigate that $r(E) = 2$. We show this is happen whenever p satisfy in the two following conditions:

- (1) $\exists a, b \in \mathbb{N} : p = a + b$, $a - b = \square$ and $a^2 + b^2 = \square$.
- (2) $\exists a, b \in \mathbb{N} : p = a^2 + b^2$, $(a, 2b) = 1$ and $(a \pm 2b)^2 + b^2 = \square$.

In part (3), Let $E : y^2 = x^3 - 4p^2x$, be the corresponding congruent number elliptic curve for $2p$. It is known that if $p \equiv 3, 7 \pmod{8}$ then $2p$ is congruent number (see[4]). Using the 2-descent method, we show in this two case, $r(E) = 1$. Moreover if $p \equiv 5 \pmod{8}$ then $r(E) = 0$, i.e., $2p$ is not congruent.

In part (4), Let $E : y^2 = x^3 - p^2q^2x$, be the corresponding congruent number elliptic curve for pq . It is known that if $[p \equiv 3$ and $q \equiv 5, 7 \pmod{8}]$ or $[p \equiv 1$ and $q \equiv 5, 7 \pmod{8}$ such that $(\frac{p}{q}) = -1]$ then pq is a congruent number (see[4]). Using 2-descent method, we show in this four cases, $r(E) = 1$. Moreover if $p, q \equiv 3 \pmod{8}$ then $r(E) = 0$, i.e., pq is not congruent.

In part (5), Let $E : y^2 = x^3 - 4p^2q^2x$. We know If $[p \equiv 5$ and $q \equiv 3, 7 \pmod{8}]$ or $[p \equiv 1$ and $q \equiv 3, 7 \pmod{8}$ such that $(\frac{p}{q}) = -1]$ then $2pq$ is congruent number (see[4]). Using the 2- descent method, we show in this four cases, $r(E) = 1$. Moreover if $[p, q \equiv 5 \pmod{8}]$ or $[p \equiv 1$ and $q \equiv 5 \pmod{8}$ such that $(\frac{p}{q}) = -1]$, then $r(E) = 0$, i.e., $2pq$ is not congruent.

2. 2-DESCENT METHOD

In this section we describe the 2- descent method for determining the rank of an elliptic curve, (see [2], Chapter 8 for more details). Let $E(\mathbb{Q})$ is the

group of rational points on the elliptic curve $E : y^2 = x^3 + ax^2 + bx$, where $a, b \in \mathbb{Q}$. Let \mathbb{Q}^* is the multiplicative group of nonzero rational numbers and \mathbb{Q}^{*2} is the subgroup of squares of elements of \mathbb{Q}^* . Define the 2-descent homomorphism α from $E(\mathbb{Q})$ to $\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ as follows :

$$\alpha(P) = \begin{cases} 1 & (\text{mod } \mathbb{Q}^{*2}) & \text{if } P = \mathcal{O} = \infty, \\ b & (\text{mod } \mathbb{Q}^{*2}) & \text{if } P = (0, 0), \\ x & (\text{mod } \mathbb{Q}^{*2}) & \text{if } P = (x, y), x \neq 0. \end{cases}$$

Similarly, take the isogenous curve $\overline{E} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$ with the group of rational points $\overline{E}(\mathbb{Q})$. The 2-descent homomorphism $\overline{\alpha}$ from $\overline{E}(\mathbb{Q})$ to $\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ as follows :

$$\overline{\alpha}(P) = \begin{cases} 1 & (\text{mod } \mathbb{Q}^{*2}) & \text{if } \overline{P} = \mathcal{O} = \infty, \\ a^2 - 4b & (\text{mod } \mathbb{Q}^{*2}) & \text{if } \overline{P} = (0, 0), \\ x & (\text{mod } \mathbb{Q}^{*2}) & \text{if } \overline{P} = (x, y), x \neq 0. \end{cases}$$

The rank of $E(\mathbb{Q})$ which is denoted by r is determined by

$$(2.1) \quad 2^r = \frac{|Im\alpha| \cdot |Im\overline{\alpha}|}{4}.$$

The group $\alpha(E(\mathbb{Q}))$ equals to the classes modulo squares of 1, b and the positive and negative divisors of b such that

$$N^2 = b_1 m^4 + a m^2 e^2 + \frac{b}{b_1} e^4,$$

$$\gcd(m, e) = \gcd(m, N) = \gcd(e, N) = \gcd(b_1, m) = \gcd\left(\frac{b}{b_1}, e\right) = 1, me \neq 0.$$

If (m, N, e) is a solution, then $P = \left(\frac{b_1 m^2}{e^2}, \frac{b_1 m N}{e^3}\right)$ belongs to $E(\mathbb{Q})$ and we have the same for $\overline{\alpha}$ as well.

3. OUR RESULTS

Part (1).

According the 2-descent method, for the elliptic curves

$$(3.1) \quad E : y^2 = x^3 - p^2 x$$

and

$$(3.2) \quad \overline{E} : y^2 = x^3 + 4p^2 q^2 x.$$

We have respectively $\{\pm 1\} \subseteq Im\alpha \subseteq \{\pm 1, \pm p\}$ and $\{1\} \subseteq Im\overline{\alpha} \subseteq \{1, 2, p, 2p\}$.

Therefore, according to (2.1), the maximum rank of (3.1) is 2. Moreover, the homogeneous equation of E is

$$(a_1) : N^2 = \pm(pm^4 - pe^4), \quad \gcd(m, pe) = \gcd(e, pm) = \gcd(N, me) = 1,$$

and the homogeneous equations of \overline{E} are

$$(b_1) : N^2 = pm^4 + 4pe^4, \quad \gcd(m, 2pe) = \gcd(e, pm) = \gcd(N, me) = 1,$$

$$(b_2) : N^2 = 2m^4 + 2p^2e^4, \quad \gcd(m, 2pe) = \gcd(e, 2m) = \gcd(N, me) = 1,$$

$$(b_3) : N^2 = 2pm^4 + 2pe^4, \quad \gcd(m, 2pe) = \gcd(e, 2pm) = \gcd(N, me) = 1.$$

First we study the solvability of the above homogeneous equations.

Proposition 3.1. *If (b_1) has integer solution then $p \equiv 1 \pmod{4}$.*

Proof. If (b_1) has integer solution then $N^2 = p(m^4 + 4e^4)$, $\gcd(m, p) = 1$. There is an integer u such that $pu^2 = m^4 + 4e^4$. Hence $m^4 \equiv -4e^4 \pmod{p}$. Therefore $(2e^2m^{*2})^2 \equiv -1 \pmod{p}$. So $(\frac{-1}{p}) = +1$, i.e., $p \equiv 1 \pmod{4}$. \square

Proposition 3.2. *If (b_2) has integer solution then $p \equiv \pm 1 \pmod{8}$.*

Proof. If (b_2) has integer solution then $N^2 = 2(m^4 + p^2e^4)$, $\gcd(m, p) = 1$. There is an integer u such that $2u^2 = m^4 + p^2e^4$. So $2u^2 \equiv m^4 \pmod{p}$. Hence $(2um^{*2})^2 \equiv 2 \pmod{p}$. So $(\frac{2}{p}) = +1$, i.e., $p \equiv \pm 1 \pmod{8}$. \square

Remark 3.3. If u is an integer number then $u^2 \equiv 0, 1, 4 \pmod{8}$. Hence, $\gcd(u, 8) = 1$ if and only if $u^2 \equiv 1 \pmod{8}$.

Proposition 3.4. *If (b_3) has integer solution then $p \equiv 1 \pmod{8}$.*

Proof. If (b_3) has integer solution then $N^2 = 2p(m^4 + e^4)$, $\gcd(em, 2) = 1$. There is an integer u such that $2pu^2 = m^4 + e^4$. Hence $2pu^2 \equiv 2 \pmod{16}$. So $pu^2 \equiv 1 \pmod{8}$. We have $(u, 8) = 1$. Therefore $u^2 \equiv 1 \pmod{8}$. Consequently $p \equiv 1 \pmod{8}$. \square

Corollary 3.5. *The above propositions are summarized in the followings:*

- (1) $\pm p \in \text{Im}\alpha$ if and only if (a_1) has integer solution.
- (2) $p \in \text{Im}\overline{\alpha}$ if and only if (b_1) has integer solution. In this case $p \equiv 1, 5 \pmod{8}$.
- (3) $2 \in \text{Im}\overline{\alpha}$ if and only if (b_2) has integer solution. In this case $p \equiv 1, 7 \pmod{8}$.
- (4) $2p \in \text{Im}\overline{\alpha}$ if and only if (b_3) has integer solution. In this case $p \equiv 1 \pmod{8}$.

Corollary 3.6. *By using previous corollary, we have:*

- (1) Let $p \equiv 3 \pmod{8}$.

Then $(b_1), (b_2), (b_3)$ do not have any integer solutions, so $\text{Im}\overline{\alpha} = \{1\}$.

As (2.1), implies $|\text{Im}\alpha| \geq 4$.

So $Im\alpha = \{\pm 1, \pm p\}$. Hence $r = 0$, i.e., p is not a congruent.

(2) Let $p \equiv 5 \pmod{8}$.

It is possible for (b_1) to have integer solution. So $Im\bar{\alpha} \subseteq \{1, p\}$.

p is a congruent number, (see [4]), we have $r \geq 1$.

As (2.1), implies $Im\alpha = \{\pm 1, \pm p\}$ and $Im\bar{\alpha} = \{1, p\}$. Hence $r = 1$.

(3) Let $p \equiv 7 \pmod{8}$.

It is possible for (b_2) to have integer solution. So $Im\bar{\alpha} \subseteq \{1, 2\}$.

p is a congruent number, (see [4]), we have $r \geq 1$.

As (2.1), $Im\alpha = \{\pm 1, \pm p\}$ and $Im\bar{\alpha} = \{1, 2\}$. Hence $r = 1$.

Part (2).

In this section, for $p \equiv 1 \pmod{8}$ we investigate that $r(E) = 2$.

- First we study the solvability of the homogeneous equation (b_1) . We need some definitions.

Definition 3.7. p is a α_- Pythagorean whenever, there are coprime integer numbers a, b and c such that $pc^2 = a^2 + b^2$.

Definition 3.8. p is a α_- Pythagorean whenever there are coprime integers a, b and c such that $pc^2 = a^2 + b^2$ and $(a - 2b)^2 + b^2 = \square$.

Definition 3.9. p is a α^+ Pythagorean whenever there are coprime integers a, b and c such that $pc^2 = a^2 + b^2$ and $(a + 2b)^2 + b^2 = \square$.

Definition 3.10. p is a α^\pm Pythagorean whenever p is a α_- Pythagorean or α^+ Pythagorean.

Remark 3.11. Considering the results of part 2, we know $p \equiv 5 \pmod{8}$ is α^\pm Pythagorean.

Example 3.12. 37 with $(a, b, c) = (22, 21, 5)$ is a α_- Pythagorean.

Example 3.13. 41 with $(a, b, c) = (5, 4, 1)$ is a α_- Pythagorean.

Example 3.14. 149 with $(a, b, c) = (10, 7, 1)$ is a α^+ Pythagorean.

Proposition 3.15. (b_1) has integer solution if and only if p is a α^\pm Pythagorean.

Proof. If (b_1) has integer solution then $N^2 = p(m^4 + 4e^4)$, $\gcd(m, 2e) = 1$.

There is an integer number u such that $pu^2 = m^4 + 4e^4$.

$$pu^2 = (m^2 - 2me + 2e^2)(m^2 + 2me + 2e^2).$$

As $\gcd(m^2 - 2me + 2e^2, m^2 + 2me + 2e^2) = 1$, there are coprime integers c and w such that

- (1) $m^2 - 2me + 2e^2 = pc^2$ and $m^2 + 2me + 2e^2 = w^2$. So $(m-e)^2 + e^2 = pc^2$ and $[(m-e) + 2e]^2 + e^2 = w^2$. Hence p is a α^+ Pythagorean.
- (2) $m^2 - 2me + 2e^2 = w^2$ and $m^2 + 2me + 2e^2 = pc^2$. So $(m+e)^2 + e^2 = pc^2$ and $[(m+e) - 2e]^2 + e^2 = w^2$. Hence p is a α^- Pythagorean. \square

Remark 3.16. If $p \equiv 1 \pmod{4} \equiv 1, 5 \pmod{8}$ then there are unique positive integers a and b such that $p = a^2 + b^2$.

$p \equiv 1 \pmod{8}$ if and only if there are unique integers k and t such that $p = 16k^2 + t^2, (t, 2k) = 1$.

$p \equiv 5 \pmod{8}$ if and only if there are unique integers k and t such that $p = 4k^2 + t^2, (t, 2k) = (k, 2) = 1$.

Lemma 3.17. If p with (a, b, c) is a α^\pm Pythagorean, then

$$a^2 \equiv 1, b^2 \equiv 0 \pmod{8} \quad \text{or} \quad a^2 \equiv 4, b^2 \equiv 1 \pmod{8}.$$

Proof. We have $pc^2 = a^2 + b^2, (a, b) = 1$ and $(a \pm 2b)^2 + b^2 = \square$.

Since pc^2 is sum of two primitive squares, then p and all factors of c are form $4k + 1$, where k is integer, (see[10]). We know squares in mod 8 are 0, 1 or 4.

Suppose otherwise if $a^2 \equiv 0, b^2 \equiv 1$ or $a^2 \equiv 1, b^2 \equiv 4 \pmod{8}$, then $\square = a^2 + 5b^2 \pm 4ab \equiv 5 \pmod{8}$, which is a contradiction. \square

Corollary 3.18. Suppose p is a α^\pm Pythagorean:

- (1) If $p = 4k^2 + t^2 \equiv 5 \pmod{8}$, then $a = 2k$ and $b = t$, where kt is odd.
- (2) If $p = 16k^2 + t^2 \equiv 1 \pmod{8}$, then $a = t$ and $b = 4k$, where t is odd.

• Next theorem tell us that the prime number $p \equiv 1 \pmod{8}$ is a α^\pm Pythagorean if and only if $c = 1$, (see the above Definition).

Theorem 3.19. (1) If $p = a^2 + b^2$ and $2 \parallel b$, then p is congruent number.

(2) If $4 \mid b$ and $(a \pm 2b)^2 + b^2 \neq \square$, then p is not a α^\pm Pythagorean.

Proof. (1) If $2 \parallel b$, then there is odd integer number b_0 such that $b = 2b_0$. So $p = a^2 + 4b_0^2 \equiv 5 \pmod{8}$, therefore p is congruent number, (see[4]).

(2) If $4 \mid b$, $(a \pm 2b)^2 + b^2 \neq \square$ and Suppose otherwise p is a α^\pm Pythagorean then there are coprime integers a_0, b_0 and $c_0 \neq 1$ such that

$$pc_0^2 = a_0^2 + b_0^2 \quad \text{and} \quad 4a_0^2 + 5b_0^2 \pm 4a_0b_0 = \square.$$

Therefore pc_0^2 is sum of two primitive numbers, then p and all factors of c_0^2 are form $4k + 1$. Consequently there are integers m and n such that m is odd number and n is nonzero even number such that $c_0^2 = m^2 + n^2$, then

$$pc_0^2 = (b^2 + a^2)(m^2 + n^2) = (bm + an)^2 + (bn - am)^2.$$

We have $[a_0 = bm + an, b_0 = bn - am]$ or $[a_0 = bm - an, b_0 = bn + am]$.

If $a_0 = bm + an$ and $b_0 = bn - am$, then $a^2n^2 \pm 5a^2m^2 \equiv \square \pmod{8}$.

If $n^2 \equiv 4$ and $m^2 \equiv 1 \pmod{8}$, then $c_0^2 \equiv 5 \pmod{8}$, which is a contradiction.

If $n^2 \equiv 0, m^2 \equiv 1$ and $a^2 \equiv 1 \pmod{8}$, then $\square \equiv \pm 5 \pmod{8}$, which is a contradiction.

proof for $a_0 = bm - an$ and $b_0 = bn + am$ is similar. \square

Example 3.20. $17 = 16 \times 1^2 + 1^2 \equiv 0 + 1 \pmod{8}$, then $a^2 = 1$ and $b^2 = 16$. As $(a \pm 2b)^2 + b^2 \neq \square$, hence 17 is not a α^\pm Pythagorean.

Example 3.21. $41 = 16 \times 1^2 + 5^2$, with $(a, b, c) = (5, 4, 1)$, is a α^- Pythagorean.

• Now, we study the solvability of the homogeneous equation (b_2) , however we first need a definitions.

Definition 3.22. p is a β_- Pythagorean whenever there are integers a, e, m and u such that $pe^2m^2 = 2a^2 - u^2$, $pe^2 = 2a - m^2$ and $(e, m) = 1$.

Remark 3.23. Considering the results of part 2, we know $p \equiv 7 \pmod{8}$ is β_- Pythagorean.

Proposition 3.24. (b_2) has integer solution if and only if p is a β_- Pythagorean.

Proof. If (b_2) has integer solution then $N^2 = 2(m^4 + p^2e^4)$, $\gcd(m, e) = 1$.

$N^2 = 2(m^4 + p^2e^4)$ if and only if there is a integer number u such that $2u^2 = m^4 + p^2e^4$ if and only if $(m^2 + pe^2)^2 = 2(u^2 + pm^2e^2)$ if and only if there is an integer number a such that $u^2 + pm^2e^2 = 2a^2$ and $m^2 + pe^2 = 2a$. \square

• Next proposition tell us that there is a relationship between solutions (b_2) and Pythagorean triples such that difference of the two smaller sides is square.

Proposition 3.25. If $pe^2 = 2a - m^2$, then (m, e, u) , is a solution (b_2) if and only if $(a - m^2, a, u)$, is a Pythagorean triple.

Proof. $(a - m^2)^2 + a^2 = u^2$ if and only if $m^2(2a - m^2) = 2a^2 - u^2$ if and only if $[pe^2m^2 = 2a^2 - u^2$ and $pe^2 = 2a - m^2]$. \square

Remark 3.26. (a, b, u) , $a < b$ is primitive Pythagorean triple if and only if there are coprime positive integers s and t such that

$$a = s^2 - t^2, b = 2st \quad \text{or} \quad a = 2st, b = s^2 - t^2.$$

Lemma 3.27. *If $a = s^2 - t^2$, $b = 2st$, $(s, t) = 1$ and $a - b = m^2$, then there are integers x and y such that $s = 2x^2 + y^2 + 2xy$, $t = 2xy$ and $(2x, y) = 1$.*

Proof. We have $(s - t)^2 - 2t^2 = m^2$. Let $k = s - t$, therefore $2t^2 = k^2 - m^2$. From $(s, t) = 1$ we have $(k, m) = 1$. So m, k are odd and $(k - m, k + m) = 2$. Consequently, there are coprime integers x and y such that

$$k + m = 4x^2, k - m = 2y^2 \quad \text{or} \quad k - m = 4x^2, k + m = 2y^2.$$

Then $k = y^2 + 2x^2$ and $m = \pm(y^2 - 2x^2)$. Hence $t = \pm 2xy$ and $s = 2x^2 + y^2 \pm 2xy$. \square

Corollary 3.28. $a = 4x^4 + y^4 + 4x^2y^2 + 8x^3y + 4xy^3$

and

$$b = 8x^2y^2 + 8x^3y + 4xy^3.$$

Lemma 3.29. *If $a = 2st$, $b = s^2 - t^2$, $(s, t) = 1$ and $a - b = m^2$ then there are integers x and y such that $s = 2xy$, $t = 2x^2 + y^2 + 2xy$ and $(2x, y) = 1$.*

Proof. The proof is similar to the previous lemma by letting $k = s + t$. \square

Corollary 3.30. $b = -4x^4 - y^4 - 4x^2y^2 + 8x^3y + 4xy^3$

and

$$a = -8x^2y^2 + 8x^3y + 4xy^3.$$

Proposition 3.31. (b_2) has integer solution if and only if $p \square \in \text{Im}f_1 \cup \text{Im}f_2$, where

$$f_1(x, y) = 4x^4 + y^4 + 12x^2y^2 + 16x^3y + 8xy^3, (2x, y) = 1,$$

$$f_2(x, y) = -4x^4 - y^4 - 12x^2y^2 + 16x^3y + 8xy^3, (2x, y) = 1.$$

Proof. (b_2) has integer solution if and only if $pe^2 = a + b$, $a - b = m^2$ and $a^2 + b^2 = u^2$, then the above above corollaries yield the result. \square

Example 3.32. $f_1(1, 1) = 41$, $f_1(-1, 7) = 137$, $f_2(1, 1) = 7$, hence for $p = 41, 137, 7$ equation (b_2) has an integer solution.

Remark 3.33. As y is odd we have $f_1(x, y) \equiv (2x^2 + y)^2 \equiv 1 \pmod{8}$ and $f_2(x, y) \equiv -(2x^2 + y)^2 \equiv 7 \pmod{8}$.

Proposition 3.34. *If pe^2 is β_- Pythagorean then p is β_- Pythagorean.*

Proof. If pe^2 is β -Pythagorean if and only if there are integers m, E and u such that $2u^2 = m^4 + (pe^2)^2 E^4, (m, E) = 1$.

Consequently m and e are odd. If $(m, e) = d$, then d is odd and also $d^2 \mid u$. There are integers m_0, u_0 and e_0 such that $e = e_0 d$, $m = m_0 d$ and $u = u_0 d^2$. We know $(m_0, e_0) = 1$. Hence $m_0^4 + p^2(e_0 E)^4 = 2u_0^2, (m_0, e_0 E) = 1$. Consequently p is β -Pythagorean. \square

Corollary 3.35. (b_2) has an integer solution if and only if $p \in \text{Im}f_1 \cup \text{Im}f_2$.
i.e., for solving the equation (b_2) , we can choose $e = 1$.

Example 3.36. 17 is not β -Pythagorean because, there are not positive integers a and b such that $17 = a + b$, $a - b = m^2$ and $a^2 + b^2 = u^2$.

Example 3.37. $[41 = 21 + 20, 21 - 20 = \square \text{ and } 21^2 + 20^2 = \square]$, i.e., $f_1(1, 1) = 41$, therefore 41 is β -Pythagorean.

- Now, we study the solvability of the homogeneous equation (b_3) .

Proposition 3.38. If (b_3) has an integer solution, then $p \square \in \text{Im}f_3$, where $f_3(x, y) = 16x^4 + y^4 + 24x^2y^2, (2x, y) = 1$.

Proof. If (b_3) has an integer solution, then

$$N^2 = 2p(m^4 + e^4), \gcd(m, 2pe) = \gcd(e, 2p) = 1.$$

There is an integer number u such that $2pu^2 = m^4 + e^4$.

So $(m^2 - e^2)^2 = 2(pu^2 - e^2m^2)$. Again there is an integer number a such that $pu^2 - e^2m^2 = 2a^2, m^2 - e^2 = 2a$, from which one gets integers y and t such that $m - e = 2y, m + e = 2t$ and $a = 2yt$. Therefore $m = t + y$ and $e = t - y$, where y or t is odd and the other is even.

We have $pu^2 = t^4 + y^4 + 6y^2t^2$. Suppose t is even and y is odd. There is an integer x such that $t = 2x$. This yields the result. \square

Example 3.39. $f_3(1, 1) = 41, f_3(2, 1) = 353$, hence for $p = 41, 353$, the equation (b_3) has an integer solution.

Proposition 3.40. If (b_2) or (b_3) has an integer solution then equation (a) has an integer solution.

Proof. If (b_2) has an integer solution, then $N^2 = 2(p^2e^4 + m^4), (me, 2) = 1$. There is an integer number u such that $2u^2 = p^2e^4 + m^4$. Let $2c = pe^2 + m^2, 2d = pe^2 - m^2$. We have $c + d = pe^2, c - d = m^2$. This implies that $c^2 - d^2 = pe^2m^2, c^2 + d^2 = u^2$. Hence $c^4 - d^4 = p(emu)^2$.

If (b_3) has an integer solution, then $N^2 = 2p(m^4 + e^4), (me, 2) = 1$. Therefore, there is an integer number u such that $2pu^2 = m^4 + e^4$. Let

$2c = e^2 + m^2$, $2d = e^2 - m^2$. We have $c + d = e^2$, $c - d = m^2$. This implies that $c^2 - d^2 = e^2m^2$, $c^2 + d^2 = pu^2$. Hence $c^4 - d^4 = p(emu)^2$. \square

Corollary 3.41. *If (b_2) or (b_3) has an integer solution, then p is congruent.*

Proof. If (b_2) or (b_3) has an integer solution then $|Im\bar{\alpha}| \geq 2$ and $|Im\alpha| = 4$. As (2.1), we have $r(E) \geq 1$. Consequently p is a congruent number. \square

Main Theorem 3.42. *$r(E) = 2$ if and only if p is α^\pm Pythagorean and β_- Pythagorean.*

Proof. p is α^\pm Pythagorean and β_- Pythagorean if and only if $p \in Im\bar{\alpha}$ and $2 \in Im\bar{\alpha}$ if and only if (b_1) and (b_2) have integer solutions if and only if $Im\bar{\alpha} = \{1, 2, p, 2p\}$ and $Im\alpha = \{\pm 1, \pm p\}$ if and only if $r(E) = 2$. \square

Corollary 3.43. *If $p \equiv 1 \pmod{8}$ then $r(E) = 2$, whenever p satisfies in the two following conditions:*

- (1) $\exists a, b \in \mathbb{N} : p = a + b$, $a - b = \square$ and $a^2 + b^2 = \square$.
- (2) $\exists a, b \in \mathbb{N} : p = a^2 + b^2$, $(a, 2b) = 1$ and $(a \pm 2b)^2 + b^2 = \square$.

Example 3.44. For $p = 41$ we have $r(E) = 2$.

Part (3).

According to the 2-descent method, for the elliptic curves

$$(3.3) \quad E : y^2 = x^3 - 4p^2x$$

and

$$(3.4) \quad \bar{E} : y^2 = x^3 + 16p^2x.$$

We have respectively $\{\pm 1\} \subseteq Im\alpha \subseteq \{\pm 1, \pm 2, \pm p, \pm 2p\}$ and $\{1\} \subseteq Im\bar{\alpha} \subseteq \{1, 2, p, 2p\}$. Therefore, according to (2.1), the maximum rank of (3.3) is 3. In fact, we showed that $Im\bar{\alpha} \subseteq \{1, p\}$. Hence the maximum rank is 2.

The homogeneous equations of E are

$$(a_1) : N^2 = \pm(m^4 - 4pe^4), \quad \gcd(m, 2pe) = \gcd(e, p) = \gcd(N, em) = 1,$$

$$(a_2) : N^2 = \pm(2m^4 - 2p^2e^4), \quad \gcd(m, 2pe) = \gcd(e, 2) = \gcd(N, em) = 1,$$

$$(a_3) : N^2 = \pm(2pm^4 - 2pe^4), \quad \gcd(m, 2pe) = \gcd(e, 2p) = \gcd(N, em) = 1$$

and the homogeneous equations of \bar{E} are

$$(b_1) : N^2 = 2m^4 + 8p^2e^4, \quad \gcd(m, 2pe) = \gcd(e, 2) = \gcd(N, em) = 1,$$

$$(b_2) : N^2 = 2pm^4 + 8pe^4, \quad \gcd(m, 2pe) = \gcd(e, 2p) = \gcd(N, em) = 1,$$

$$(b_3) : N^2 = pm^4 + 16pe^4, \quad \gcd(m, 2pe) = \gcd(e, p) = \gcd(N, em) = 1.$$

First we study the solvability of the above homogeneous equations.

Proposition 3.45. *If (a_2) has an integer solution, then $p \equiv 1, 3, 7 \pmod{8}$.*

Proof. If (a_2) has an integer solution, then $N^2 = \pm 2(m^4 - p^2 e^4)$, $\gcd(m, p) = 1$. There is an integer number u such that $2u^2 = \pm(m^4 - p^2 e^4)$. So $2u^2 \equiv \pm m^4 \pmod{p}$. Hence $(2um^{*2})^2 \equiv \pm 2 \pmod{p}$. Implies $(\frac{\pm 2}{p}) = +1$, i.e., $p \equiv 1, 3, 7 \pmod{8}$. \square

Proposition 3.46. *(b_1) and (b_2) do not have any integer solutions.*

Proof. If (b_1) has an integer solution, then $N^2 = 2(m^4 + 4p^2 e^4)$, $\gcd(m, 2) = 1$. There is an integer number u such that $2u^2 = m^4 + 4p^2 e^4$. So m is an even number, which is a contradiction.

If (b_2) has an integer solution, then $N^2 = 2p(m^4 + 4e^4)$, $\gcd(m, 2) = 1$.

There is an integer number u such that $2pu^2 = m^4 + 4e^4$. So m is an even number, which is a contradiction. \square

Proposition 3.47. *If (b_3) has an integer solution, then $p \equiv 1 \pmod{8}$.*

Proof. If (b_3) has integer solution, then $N^2 = p(m^4 + 16e^4)$, $\gcd(m, 2) = 1$. There is an integer number u such that $pu^2 = m^4 + 16e^4$.

We have $pu^2 \equiv 1 \pmod{8}$. So $(u, 8) = 1$. Therefore $u^2 \equiv 1 \pmod{8}$. Consequently $p \equiv 1 \pmod{8}$. \square

Corollary 3.48. *The above propositions are summarized in the followings:*

- (1) $\pm p \in \text{Im}\alpha$ if and only if (a_1) has an integer solution.
- (2) $\pm 2 \in \text{Im}\alpha$ if and only if (a_2) has an integer solution. In this case, $p \equiv 1, 3, 7 \pmod{8}$.
- (3) $\pm 2p \in \text{Im}\alpha$ if and only if (a_3) has an integer solution.
- (4) $2 \notin \text{Im}\bar{\alpha}$, i.e., (b_1) does not have an integer solution.
- (5) $2p \notin \text{Im}\bar{\alpha}$, i.e., (b_2) does not have an integer solution.
- (6) $p \in \text{Im}\bar{\alpha}$ if and only if (b_3) has an integer solution. In this case, $p \equiv 1 \pmod{8}$.

Corollary 3.49. *By using the previous corollary, we have:*

- (1) Let $p \equiv 5 \pmod{8}$.
 (b_3) does not have integer solutions, then $\text{Im}\bar{\alpha} = \{1\}$.
It is possible for (a_1) and (a_3) to have integer solutions. So $\text{Im}\alpha \subseteq \{\pm 1, \pm p\}$ or $\{\pm 1, \pm 2p\}$.
As (2.1), implies $|\text{Im}\alpha| \geq 4$. Therefore $\text{Im}\alpha = \{\pm 1, \pm p\}$ or $\{\pm 1, \pm 2p\}$. Hence $r = 0$, i.e., $2p$ is not congruent.

(2) Let $p \equiv 3, 7 \pmod{8}$.

(b₃) does not have integer solutions, then $Im\bar{\alpha} = \{1\}$.

It is possible for (a_1) , (a_2) and (a_3) to have integer solutions, then $Im\alpha \subseteq \{\pm 1, \pm 2, \pm p, \pm 2p\}$.

$2p$ is congruent, (see[4]), so $r \geq 1$.

The equation (2.1), implies that $|Im\alpha| \geq 8$. Therefore $Im\alpha = \{\pm 1, \pm 2, \pm p, \pm 2p\}$. Hence $r = 1$.

part (4).

According to the 2-descent method, for the elliptic curves

$$(3.5) \quad E : y^2 = x^3 - p^2 q^2 x$$

and

$$(3.6) \quad \bar{E} : y^2 = x^3 + 4p^2 q^2 x.$$

We have respectively $\{\pm 1\} \subseteq Im\alpha \subseteq \{\pm 1, \pm p, \pm q \pm pq\}$ and $\{1\} \subseteq Im\bar{\alpha} \subseteq \{1, 2, p, q, pq, 2p, 2q, 2pq\}$. Therefore, according to (2.1), the maximum rank of (3.5) is 4. Moreover, the homogeneous equations of E are

$$(a_1) : N^2 = \pm(pm^4 - pq^2e^4), \quad \gcd(m, pqe) = \gcd(e, pm) = \gcd(N, me) = 1,$$

$$(a_2) : N^2 = \pm(qm^4 - p^2qe^4), \quad \gcd(m, pqe) = \gcd(e, qm) = \gcd(N, me) = 1,$$

$$(a_3) : N^2 = \pm(pqm^4 - pqe^4), \quad \gcd(m, pqe) = \gcd(e, pqm) = \gcd(N, me) = 1,$$

and the homogeneous equations of \bar{E} are

$$(b_1) : N^2 = pm^4 + 4pq^2e^4, \quad \gcd(m, 2pqe) = \gcd(e, pm) = \gcd(N, me) = 1,$$

$$(b_2) : N^2 = qm^4 + 4p^2qe^4, \quad \gcd(m, 2pqe) = \gcd(e, qm) = \gcd(N, me) = 1,$$

$$(b_3) : N^2 = 2m^4 + 2p^2q^2e^4, \quad \gcd(m, 2pqe) = \gcd(e, 2m) = \gcd(N, me) = 1,$$

$$(b_4) : N^2 = 2pm^4 + 2pq^2e^4, \quad \gcd(m, 2pqe) = \gcd(e, 2pm) = \gcd(N, me) = 1,$$

$$(b_5) : N^2 = 2qm^4 + 2p^2qe^4, \quad \gcd(m, 2pqe) = \gcd(e, 2qm) = \gcd(N, me) = 1,$$

$$(b_6) : N^2 = pqm^4 + 4pqe^4, \quad \gcd(m, 2pqe) = \gcd(e, pqm) = \gcd(N, me) = 1,$$

$$(b_7) : N^2 = 2pqm^4 + 2pqe^4, \quad \gcd(m, 2pqe) = \gcd(e, 2pqm) = \gcd(N, me) = 1.$$

Equations (a_1) , (a_2) and (b_1) , (b_2) and (b_4) , (b_5) are the same.

First we study the solvability of these homogeneous equations.

Proposition 3.50. *If (a_1) has an integer solution, then $[p \text{ or } q \equiv 1, 3, 7 \pmod{8} \text{ and } (\frac{-q}{p}) = +1]$ or $[p \text{ or } q \equiv 1, 7 \pmod{8} \text{ and } (\frac{q}{p}) = +1]$.*

Proof. If (a_1) has an integer solution, then $N^2 = \pm p(m^4 - q^2 e^4)$, $\gcd(m, Nepq) = 1$. There is an integer number u such that $\pm pu^2 = m^4 - q^2 e^4$.

If $q \mid u$, then $q \mid m$. From $N = pu$, we have $\gcd(N, m) \neq 1$, a contradiction. So $\gcd(q, u) = 1$.

There are positive integers u_1, u_2 and a square free t such that

$$m^2 + qe^2 = pu_1^2 t \quad \text{and} \quad m^2 - qe^2 = \pm u_2^2 t,$$

or

$$m^2 - qe^2 = \pm pu_1^2 t \quad \text{and} \quad m^2 + qe^2 = u_2^2 t.$$

We have $2m^2 = \pm t(pu_1^2 \pm u_2^2)$ and $2qe^2 = \mp t(pu_1^2 \mp u_2^2)$. So $t \mid 2m^2$ and $t \mid 2qe^2$.

Suppose t is odd number. As $t \mid m^2$, we have $\gcd(m, t) \neq 1$. So $\gcd(t, e) = 1$. From $t \mid qe^2$ we have $t \mid q$. Because $u = u_1 u_2 t$ and $\gcd(q, u) = 1$, we have $t = 1$, which is a contradiction. Therefore $t = 1$.

(1) If $m^2 + qe^2 = pu_1^2$ and $m^2 - qe^2 = \pm u_2^2$ then $2m^2 = pu_1^2 \pm u_2^2$.

From $m^2 + qe^2 = pu_1^2$ we have, $(\frac{-q}{p}) = +1$.

From $2m^2 = pu_1^2 \pm u_2^2$ we have, $(\frac{\pm 2}{p}) = +1$, i.e., $p \equiv 1, 3, 7 \pmod{8}$.

(2) If $m^2 - qe^2 = \pm pu_1^2$ and $m^2 + qe^2 = u_2^2$ then $2m^2 = \pm pu_1^2 + u_2^2$.

From $m^2 - qe^2 = \pm pu_1^2$, we have $(\frac{q}{p}) = +1$.

From $2m^2 = \pm pu_1^2 + u_2^2$, we have $(\frac{2}{p}) = +1$, i.e., $p \equiv 1, 7 \pmod{8}$.

Now, we suppose t is even. If $t = 2k$, where $k \neq 1$ is odd number, then $m^2 = \pm k(pu_1^2 \pm u_2^2)$ and $qe^2 = \mp k(pu_1^2 \mp u_2^2)$. So $k \mid m^2$ and $k \mid qe^2$, as above we have a contradiction. Hence $t = 2$.

(3) If $m^2 + qe^2 = 2pu_1^2$ and $m^2 - qe^2 = \pm 2u_2^2$ then $qe^2 = pu_1^2 \pm u_2^2$.

From $m^2 + qe^2 = 2pu_1^2$, we have $(\frac{-q}{p}) = +1$.

$m^2 - qe^2 = \pm 2u_2^2$, so $(\frac{\pm 2}{q}) = +1$, i.e., $q \equiv 1, 3, 7 \pmod{8}$.

(4) If $m^2 - qe^2 = \pm 2pu_1^2$ and $m^2 + qe^2 = 2u_2^2$ then $qe^2 = u_2^2 \mp pu_1^2$.

From $m^2 + qe^2 = 2u_2^2$, we have $(\frac{2}{q}) = +1$, i.e., $q \equiv 1, 7 \pmod{8}$.

From $qm^2 = u_2^2 \pm pu_1^2$, we have $(\frac{q}{p}) = +1$. \square

Proposition 3.51. *If (b_1) has an integer solution, then $p \equiv 1 \pmod{4}$ and $(\frac{p}{q}) = +1$.*

Proof. If (b_1) has an integer solution, then $N^2 = p(m^4 + 4q^2 e^4)$, $\gcd(m, pq) = 1$. There is an integer number u such that $pu^2 = m^4 + 4q^2 e^4$.

$m^4 \equiv -4q^2 e^4 \pmod{p}$, so $(2qe^2 m^{*2})^2 \equiv -1 \pmod{p}$. Hence $(\frac{-1}{p}) = +1$, i.e., $p \equiv 1 \pmod{4}$.

$pu^2 \equiv m^4 \pmod{q}$, so $(m^{*2}pu)^2 \equiv p \pmod{q}$, i.e., $(\frac{p}{q}) = +1$. \square

Proposition 3.52. *If (b_3) has an integer solution, then $p, q \equiv \pm 1 \pmod{8}$.*

Proof. If (b_3) has an integer solution then $N^2 = 2(m^4 + p^2q^2e^4)$, $\gcd(m, pq) =$

1. There is an integer number u such that $2u^2 = m^4 + p^2q^2e^4$.

$2u^2 \equiv m^4 \pmod{p}$, so $(m^{*2}2u)^2 \equiv 2 \pmod{p}$. This implies that $(\frac{2}{p}) = +1$, i.e., $p \equiv \pm 1 \pmod{8}$.

$2u^2 \equiv m^4 \pmod{q}$, so $(m^{*2}2u)^2 \equiv 2 \pmod{q}$. This implies that $(\frac{2}{q}) = +1$, i.e., $q \equiv \pm 1 \pmod{8}$. \square

Proposition 3.53. *If (b_4) has an integer solution, then $p \equiv 1 \pmod{4}$ and $(\frac{2p}{q}) = +1$.*

Proof. If (b_4) has an integer solution, then $N^2 = 2p(m^4 + q^2e^4)$, $\gcd(m, pq) =$

1. There is an integer u such that $2pu^2 = m^4 + q^2e^4$.

$2pu^2 \equiv m^4 \pmod{q}$, so $(m^{*2}2pu)^2 \equiv 2p \pmod{q}$, i.e., $(\frac{2p}{q}) = +1$.

$-m^4 \equiv q^2e^4 \pmod{p}$, so $(qe^2m^{*2})^2 \equiv -1 \pmod{p}$. Hence $(\frac{-1}{p}) = +1$, i.e., $p \equiv 1 \pmod{4}$. \square

Proposition 3.54. *If (b_6) has an integer solution. then $p, q \equiv 1 \pmod{4}$.*

Proof. If (b_6) has an integer solution, then $N^2 = pq(m^4 + 4e^4)$, $\gcd(m, 2pq) =$

1. There is an integer number u such that $pqu^2 = m^4 + 4e^4$.

$-m^4 \equiv 4e^4 \pmod{p}$, so $(2e^2m^{*2})^2 \equiv -1 \pmod{p}$. Hence $(\frac{-1}{p}) = +1$, i.e., $p \equiv 1 \pmod{4}$.

$-m^4 \equiv 4e^4 \pmod{q}$, so $(2e^2m^{*2})^2 \equiv -1 \pmod{q}$. Hence $(\frac{-1}{q}) = +1$, i.e., $q \equiv 1 \pmod{4}$. \square

Finally we verify (b_7) . First we prove the following lemma.

Remark 3.55. If b is a quadratic residue, then obviously b^* is a quadratic residue. Moreover if -1 is a quadratic residue then $-b$ is a quadratic residue too.

Remark 3.56. -1 is a quadratic residue if and only if $p \equiv 1 \pmod{4}$, i.e., $p \equiv 1, 5 \pmod{8}$.

Lemma 3.57. *If there is an integer number x such that $x^4 \equiv -1 \pmod{p}$ then $p \equiv 1 \pmod{8}$.*

Proof. $\frac{p-1}{2}$ number are quadratic residues and the same number of non-residues.

If $p = 8k + 5$, then there are $4k + 2$ quadratic residues.

$$x^2 \equiv \pm b \pmod{8} \iff x^4 \equiv b^2 \pmod{8}.$$

Therefore, there are $2k + 1$ residues of degree 4. So there are $2k$ residues of degree 4 except 1. If $b \neq \pm 1$ is a residue, then $b^* \neq b$ and b^* is a residue as well. Moreover only ± 1 equal to their inverse in every mod. Putting these together, one can get that -1 is not residue of degree 4. \square

Proposition 3.58. *If (b_7) has an integer solution, then $p, q \equiv 1 \pmod{8}$.*

Proof. If (b_7) has an integer solution, then $N^2 = 2pq(m^4 + e^4)$, $\gcd(m, pq) = 1$. There is integer number u such that $2pqu^2 = m^4 + e^4$.

$$-m^4 \equiv e^4 \pmod{p}, \text{ so } (em^*)^4 \equiv -1 \pmod{p}, \text{ i.e., } p \equiv 1 \pmod{8}.$$

$$-m^4 \equiv e^4 \pmod{q}, \text{ so } (em^*)^4 \equiv -1 \pmod{q}, \text{ i.e., } q \equiv 1 \pmod{8}. \quad \square$$

Corollary 3.59. *The above propositions are summarized in the following statements.*

- (1) $p \in Im\alpha$ if and only if (a_1) has an integer solution. In this case,
 p or $q \equiv 1, 3, 7 \pmod{8}$ and $\left(\frac{-q}{p}\right) = +1$
or
 p or $q \equiv 1, 7 \pmod{8}$ and $\left(\frac{q}{p}\right) = +1$.
- (2) $q \in Im\alpha$ if and only if (a_2) has an integer solution. In this case,
 p or $q \equiv 1, 3, 7 \pmod{8}$ and $\left(\frac{-p}{q}\right) = +1$
or
 p or $q \equiv 1, 7 \pmod{8}$ and $\left(\frac{p}{q}\right) = +1$.
- (3) $pq \in Im\alpha$ if and only if (a_3) has an integer solution.
- (4) $p \in Im\bar{\alpha}$ if and only if (b_1) has an integer solution. In this case,
 $p \equiv 1, 5 \pmod{8}$ and $\left(\frac{p}{q}\right) = +1$.
- (5) $q \in Im\bar{\alpha}$ if and only if (b_2) has an integer solution. In this case,
 $q \equiv 1, 5 \pmod{8}$ and $\left(\frac{q}{p}\right) = +1$.
- (6) $2 \in Im\bar{\alpha}$ if and only if (b_3) has an integer solution. In this case,
 $p, q \equiv 1, 7 \pmod{8}$.
- (7) $2p \in Im\bar{\alpha}$ if and only if (b_4) has an integer solution. In this case,
 $p \equiv 1, 5, q \equiv 1, 7 \pmod{8}$ and $\left(\frac{p}{q}\right) = +1$
or
 $p \equiv 1, 5, q \equiv 3, 5 \pmod{8}$ and $\left(\frac{p}{q}\right) = -1$.
- (8) $2q \in Im\bar{\alpha}$ if and only if (b_5) has an integer solution' In this case,
 $q \equiv 1, 5, p \equiv 1, 7 \pmod{8}$ and $\left(\frac{q}{p}\right) = +1$
or
 $q \equiv 1, 5, p \equiv 3, 5 \pmod{8}$ and $\left(\frac{q}{p}\right) = -1$.
- (9) $pq \in Im\bar{\alpha}$ if and only if (b_6) has an integer solution. In this case,
 $p, q \equiv 1, 5 \pmod{8}$.

(10) $2pq \in Im\bar{\alpha}$ if and only if (b_7) has an integer solution. In this case,
 $p, q \equiv 1 \pmod{8}$.

Corollary 3.60. *By the previous corollary, we have:*

(1) Let $p, q \equiv 3 \pmod{8}$.

$(b_i), 1 \leq i \leq 7$, does not have an integer solution. So $Im\bar{\alpha} = \{1\}$.

As (2.1), then $|Im\alpha| \geq 4$.

It is possible for $(a_1), (a_2)$ and (a_3) to have integer solutions. If (a_1) and (a_2) have integer solutions, then $\left(\frac{q}{p}\right) = -1$ and $\left(\frac{p}{q}\right) = -1$. By using quadratic reciprocity, which is a contradiction. Therefore $Im\alpha \subseteq \{\pm 1, \pm p\}, \{\pm 1, \pm q\}$ or $\{\pm 1, \pm pq\}$.

Consequently, $Im\alpha = \{\pm 1, \pm p\}, \{\pm 1, \pm q\}$ or $\{\pm 1, \pm pq\}$.

Hence $r = 0$, i.e., pq is not congruent.

(2) Let $p \equiv 3, q \equiv 5 \pmod{8}$.

It is possible for (b_2) or (b_5) to have an integer solution. Therefore $Im\bar{\alpha} \subseteq \{1, q\}$ or $\{1, 2q\}$.

It is possible for (a_3) to have an integer solution, then $Im\alpha \subset \{\pm 1, \pm pq\}$. As pq is congruent number, (see[4]). So $r \geq 1$.

As (2.1), implies that $Im\alpha = \{\pm 1, \pm pq\}$ and $Im\bar{\alpha} = \{1, q\}$ or $\{1, 2q\}$. Hence $r = 1$.

(3) Let $p \equiv 3, q \equiv 7 \pmod{8}$.

$(b_i), 1 \leq i \leq 7$, does not have an integer solution. So $Im\bar{\alpha} = \{1\}$.

It is possible for $(a_1), (a_2)$ and (a_3) to have integer solutions. So $Im\alpha \subseteq \{\pm 1, \pm p, \pm q, \pm pq\}$.

As pq is congruent number, (see[4]), so $r \geq 1$.

As (2.1), implies that $Im\alpha = \{\pm 1, \pm p, \pm q, \pm pq\}$. Hence $r = 1$.

(4) Let $p \equiv 1, q \equiv 5 \pmod{8}$ and $\left(\frac{p}{q}\right) = -1$.

It is possible for (a_3) to have an integer solution. Therefore, $Im\alpha \subseteq \{\pm 1, \pm pq\}$.

It is possible for (b_4) or (b_6) to have an integer solution. Therefore, $Im\bar{\alpha} \subseteq \{1, 2p\}$ or $\{1, pq\}$.

As pq is congruent number, (see[4]), we have $r \geq 1$.

As (2.1), Implies that $Im\bar{\alpha} = \{1, 2p\}$ or $\{1, pq\}$ and $Im\alpha = \{\pm 1, \pm pq\}$. Hence $r = 1$.

(5) Let $p \equiv 1, q \equiv 7 \pmod{8}$ and $\left(\frac{p}{q}\right) = -1$.

It is possible for (a_2) or (a_3) to have an integer solution. Therefore, $Im\alpha \subseteq \{\pm 1, \pm q\}$ or $\{\pm 1, \pm pq\}$.

It is possible for (b_3) to have an integer solution. Then $Im\bar{\alpha} \subseteq \{1, 2\}$.

As pq is a congruent number, (see[4]), we have $r \geq 1$.

As (2.1), Implies that $Im\alpha = \{\pm 1, \pm q\}$ or $\{\pm 1, \pm pq\}$ and $Im\bar{\alpha} = \{1, 2\}$. Hence $r = 1$.

part (5).

According to the 2-descent method, for the elliptic curves

$$(3.7) \quad E : y^2 = x^3 - 4p^2q^2x$$

and

$$(3.8) \quad \bar{E} : y^2 = x^3 + 16p^2q^2x.$$

We have respectively $\{\pm 1\} \subseteq Im\alpha \subseteq \{\pm 1, \pm 2, \pm p, \pm q, \pm pq, \pm 2p, \pm 2q, \pm 2pq\}$ and $\{1\} \subseteq Im\bar{\alpha} \subseteq \{1, 2, p, q, pq, 2p, 2q, 2pq\}$. Therefore, according to (2.1), the maximum rank of (3.7) is 5. Moreover, the homogeneous equations of E are

$$(a_1) : N^2 = \pm(2m^4 - 2p^2q^2e^4), \quad \gcd(m, 2pqe) = \gcd(e, 2m) = \gcd(N, me) = 1,$$

$$(a_2) : N^2 = \pm(pm^4 - 4pq^2e^4), \quad \gcd(m, 2pqe) = \gcd(e, pm) = \gcd(N, me) = 1,$$

$$(a_3) : N^2 = \pm(qm^4 - 4p^2qe^4), \quad \gcd(m, 2pqe) = \gcd(e, qm) = \gcd(N, me) = 1,$$

$$(a_4) : N^2 = \pm(2pm^4 - 2p^2q^2e^4), \quad \gcd(m, 2pqe) = \gcd(e, 2pm) = \gcd(N, me) = 1,$$

$$(a_5) : N^2 = \pm(2qm^4 - 2p^2qe^4), \quad \gcd(m, 2pqe) = \gcd(e, 2qm) = \gcd(N, me) = 1,$$

$$(a_6) : N^2 = \pm(pqm^4 - 4pqe^4), \quad \gcd(m, 2pqe) = \gcd(e, pqm) = \gcd(N, me) = 1,$$

$$(a_7) : N^2 = \pm(2pqm^4 - 2p^2qe^4), \quad \gcd(m, 2pqe) = \gcd(e, 2pqm) = \gcd(N, me) = 1,$$

and the homogeneous equations of \overline{E} are

$$\begin{aligned}
(b_1) : N^2 &= 2m^4 + 8p^2q^2e^4, & \gcd(m, 2pqe) &= \gcd(e, 2m) = \gcd(N, me) = 1, \\
(b_2) : N^2 &= pm^4 + 16pq^2e^4, & \gcd(m, 2pqe) &= \gcd(e, pm) = \gcd(N, me) = 1, \\
(b_3) : N^2 &= qm^4 + 16p^2qe^4, & \gcd(m, 2pqe) &= \gcd(e, qm) = \gcd(N, me) = 1, \\
(b_4) : N^2 &= 2pm^4 + 8pq^2e^4, & \gcd(m, 2pqe) &= \gcd(e, 2pm) = \gcd(N, me) = 1, \\
(b_5) : N^2 &= 2qm^4 + 8p^2qe^4, & \gcd(m, 2pqe) &= \gcd(e, 2qm) = \gcd(N, me) = 1, \\
(b_6) : N^2 &= pqm^4 + 16pqe^4, & \gcd(m, 2pqe) &= \gcd(e, pqm) = \gcd(N, me) = 1, \\
(b_7) : N^2 &= 2pqm^4 + 8pqe^4, & \gcd(m, 2pqe) &= \gcd(e, 2pqm) = \gcd(N, me) = 1.
\end{aligned}$$

The equations $(a_2), (a_3)$ and $(a_4), (a_5)$ and $(b_2), (b_3)$ and also $(b_4), (b_5)$ are similar.

First we study the solvability of the above homogeneous equations.

Proposition 3.61. *If (a_1) has an integer solution, then $p, q \equiv 1, 3, 7 \pmod{8}$.*

Proof. If (a_1) has an integer solution, then $N^2 = \pm 2(m^4 - p^2q^2e^4)$, $\gcd(m, Npq) = \gcd(me, 2) = 1$. There is an integer number u such that $\pm 2u^2 = m^4 - p^2q^2e^4$.

There are integer numbers u_1, u_2 and an odd number t such that

$$m^2 - pqe^2 = \pm 2u_1^2t \quad \text{and} \quad m^2 + pqe^2 = 4u_2^2t$$

or

$$m^2 - pqe^2 = \pm 4u_1^2t \quad \text{and} \quad m^2 + pqe^2 = 2u_2^2t.$$

We have $m^2 = \pm t(2u_1^2 \pm u_2^2)$. So $t \mid m^2$. We know $N = 2u = 2u_1u_2t$ and $(N, m) = 1$. Hence $t = 1$.

If $p \mid u_1$, from $m^2 \pm pqe^2 = \pm 4u_1^2$, we have $p \mid m$, which is a contradiction. Consequently $(p, u_1) = 1$.

We have $pqe^2 = \pm(2u_1^2 \pm u_2^2)$. Implies $\pm 2u_1^2 \equiv u_2^2 \pmod{p}$. Therefore $\pm 2 \equiv (u_2u_1^*)^2 \pmod{p}$. Consequently $(\frac{\pm 2}{p}) = +1$, i.e., $p \equiv 1, 3, 7 \pmod{8}$.

The Proof for q is similar. \square

Proposition 3.62. *If (a_2) has an integer solution, then $(\frac{\pm p}{q}) = +1 = (\frac{\pm 2q}{p})$.*

Proof. If (a_2) has an integer solution, then $N^2 = \pm p(m^4 - 4q^2e^4)$, $\gcd(m, Npq) = \gcd(e, p) = 1$. There is an integer number u such that $\pm pu^2 = m^4 - 4q^2e^4$.

So, there are positive integer numbers u_1, u_2 and t such that,

$$m^2 - 2qe^2 = \pm pu_1^2t \quad \text{and} \quad m^2 + 2qe^2 = u_2^2t$$

or

$$m^2 - 2qe^2 = \pm u_2^2 t \quad \text{and} \quad m^2 + 2qe^2 = pu_1^2 t.$$

We have $2m^2 = \pm t(pu_1^2 \pm u_2^2)$. So $t \mid 2m^2$.

(1) suppose t is odd.

We have $t \mid m^2$. Because $N = pu = pu_1 u_2 t$ and $\gcd(N, m) = 1$, consequently $t = 1$.

From $m^2 \equiv \pm 2qe^2 \pmod{p}$, we have $(me^*)^2 \equiv \pm 2q \pmod{p}$. So $\left(\frac{\pm 2q}{p}\right) = +1$.

From $m^2 \equiv \pm pu_1^2 \pmod{q}$, we have $(pm^*u_1)^2 \equiv \pm p \pmod{q}$. Consequently $\left(\frac{\pm p}{q}\right) = +1$.

(2) Now, suppose t is even.

If $t = 2k$, where k is an odd integer then $m^2 = \pm k(pu_1^2 \pm u_2^2)$. So $k \mid m^2$, similarly we have $k = 1$. Hence $t = 2$.

From $m^2 \pm 2qe^2 = \pm 2pu_1^2$, we get $m^2 \equiv \pm 2pu_1^2 \pmod{q}$. Hence $(m^*2pu_1)^2 \equiv \pm 2p \pmod{q}$. Consequently $\left(\frac{\pm 2p}{q}\right) = +1$.

From $m^2 \pm 2qe^2 = \pm 2u_2^2$, we get $m^2 \equiv \pm 2u_2^2 \pmod{q}$. Hence $\pm 2 \equiv (2m^*u_2)^2 \pmod{q}$. Consequently $\left(\frac{\pm 2}{q}\right) = +1$.

From $m^2 \pm 2qe^2 = \pm 2pu_1^2$, we get $m^2 \equiv \pm 2qe^2 \pmod{p}$. Hence $(me^*)^2 \equiv \pm 2q \pmod{p}$. Consequently $\left(\frac{\pm 2q}{p}\right) = +1$. \square

Corollary 3.63. *If $p, q \equiv 5 \pmod{8}$, then (a_2) does not have an integer solution.*

Proof. If (a_2) has an integer solution, then $\left(\frac{\pm p}{q}\right) = +1$ and $\left(\frac{\pm 2q}{p}\right) = +1$.

$\left(\frac{2q}{p}\right) = +1$ if and only if $[p \equiv 1, 7 \pmod{8} \text{ and } \left(\frac{q}{p}\right) = +1]$ or $[p \equiv 3, 5 \pmod{8} \text{ and } \left(\frac{q}{p}\right) = -1]$.

$\left(\frac{-2q}{p}\right) = +1$ if and only if $[p \equiv 1, 3 \pmod{8} \text{ and } \left(\frac{q}{p}\right) = +1]$ or $[p \equiv 5, 7 \pmod{8} \text{ and } \left(\frac{q}{p}\right) = -1]$.

If for $p, q \equiv 5 \pmod{8}$ equation (a_2) has an integer solution, then $\left(\frac{q}{p}\right) = -1$ and $\left(\frac{\pm p}{q}\right) = \left(\frac{p}{q}\right) = +1$. By the quadratic reciprocity, this is a contradiction. \square

Proposition 3.64. *If (a_4) has an integer solution, then $\left(\frac{q}{p}\right) = +1 = \left(\frac{\pm 2p}{q}\right)$.*

Proof. If (a_4) has an integer solution, then $N^2 = \pm 2p(m^4 - q^2e^4)$, $\gcd(m, 2Npqe) = 1$. There is an integer number u such that $\pm 2pu^2 = m^4 - q^2e^4$. So, there are integer numbers u_1, u_2 and a free square odd number t such that

$$m^2 + qe^2 = 2pu_1^2 t \quad \text{and} \quad m^2 - qe^2 = \pm 4u_2^2 t.$$

or

$$m^2 - qe^2 = \pm 4pu_1^2 t \quad \text{and} \quad m^2 + qe^2 = 2u_2^2 t.$$

We have $m^2 = t(pu_1^2 \pm 2u_2^2)$ or $m^2 = t(\pm 2pu_1^2 + u_2^2)$. So $t \mid m^2$. From $N = 2pu = 4pu_1u_2t$ and $(N, m) = 1$, implies $t = 1$.

(1) In case one, we have $m^2 \equiv 2pu_1^2 \pmod{q}$. So $2p \equiv (2pu_1m^*)^2 \pmod{q}$. Consequently $(\frac{2p}{q}) = +1$.

From $m^2 \equiv \pm qe^2 \pmod{p}$, we have $\pm q \equiv (qe^2m^*)^2 \pmod{p}$. consequently $(\frac{q}{p}) = +1$.

(2) In case two, we have $m^2 \equiv \pm 4pu_1^2 \pmod{q}$, implies $\pm p \equiv (2m^*pu_1)^2 \pmod{q}$. Consequently $(\frac{\pm p}{q}) = +1$.

$m^2 \equiv 2u_2^2 \pmod{q}$, so $2 \equiv (2m^*u_2)^2 \pmod{q}$, i.e., $(\frac{2}{q}) = +1$.

$m^2 \equiv qe^2 \pmod{p}$, so $(me^*)^2 \equiv q \pmod{p}$, i.e., $(\frac{q}{p}) = +1$. \square

Corollary 3.65. *If $p, q \equiv 5 \pmod{8}$, then (a_4) does not have any integer solution.*

Proof. If (a_4) has an integer solution, then $(\frac{p}{q}) = +1$, and $(\frac{\pm 2q}{p}) = +1$.

$(\frac{2q}{p}) = +1$ if and only if $[p \equiv 1, 7 \pmod{8} \text{ and } (\frac{q}{p}) = +1]$ or $[p \equiv 3, 5 \pmod{8} \text{ and } (\frac{q}{p}) = -1]$. $(\frac{-2q}{p}) = +1$ if and only if $[p \equiv 1, 3 \pmod{8} \text{ and } (\frac{q}{p}) = +1]$ or $[p \equiv 5, 7 \pmod{8} \text{ and } (\frac{q}{p}) = -1]$. If for $p, q \equiv 5 \pmod{8}$, equation (a_4) has integer solution then $(\frac{q}{p}) = -1$ and $(\frac{p}{q}) = +1$. By using quadratic reciprocity, which is a contradiction. \square

Proposition 3.66. *If (a_6) has integer solution then $p, q \equiv 1, 3, 7 \pmod{8}$.*

Proof. If (a_6) has an integer solution, then $N^2 = \pm pq(m^4 - 4e^4)$, $\gcd(e, pq) = 1$. There is an integer number u such that $\pm pq u^2 = m^4 - 4e^4$. So, there are positive integers u_1, u_2 and t such that

$$m^2 + 2e^2 = pu_1^2t \quad \text{and} \quad m^2 - 2e^2 = \pm qu_2^2t,$$

$$m^2 + 2e^2 = qu_1^2t \quad \text{and} \quad m^2 - 2e^2 = \pm pu_2^2t,$$

$$m^2 + 2e^2 = pqu_1^2t \quad \text{and} \quad m^2 - 2e^2 = \pm u_2^2t,$$

$$m^2 - 2e^2 = \pm pqu_1^2t \quad \text{and} \quad m^2 + 2e^2 = u_2^2t.$$

We have $m^2 \equiv \pm 2e^2 \pmod{p}$. Hence $(me^*)^2 \equiv \pm 2 \pmod{p}$. So $(\frac{\pm 2}{p}) = +1$, consequently $p \equiv 1, 3, 7 \pmod{8}$.

We have $m^2 \equiv \pm 2e^2 \pmod{q}$. Hence $(me^*)^2 \equiv \pm 2 \pmod{q}$. So $(\frac{\pm 2}{q}) = +1$, consequently $q \equiv 1, 3, 7 \pmod{8}$. \square

Proposition 3.67. *$(b_1), (b_4), (b_5)$ and (b_7) does not have any integer solution.*

Proof. If (b_1) has an integer solution then $N^2 = 2(m^4 + 4p^2q^2e^4)$, $(m, 2) = 1$. There is an integer number u such that $2u^2 = m^4 + 4p^2q^2e^4$. Hence m is even, which is a contradiction.

The proof for (b_4) , (b_5) and (b_7) are similar. \square

Proposition 3.68. *If (b_2) has an integer solution, then $p \equiv 1 \pmod{8}$ and $(\frac{p}{q}) = +1$.*

Proof. If (b_2) has an integer solution then $N^2 = p(m^4 + 16q^2e^4)$, $\gcd(m, 2pq) = 1$. There is an integer u such that $pu^2 = m^4 + 16q^2e^4$.

Hence $pu^2 \equiv m^4 \pmod{q}$. So $(pum^{*2})^2 \equiv p \pmod{q}$. Consequently $(\frac{p}{q}) = +1$.

We have $m^4 \equiv -16q^2e^4 \pmod{p}$. So $(4qe^2m^{*2})^2 \equiv -1 \pmod{p}$, so $(\frac{-1}{p}) = +1$, i.e., $p \equiv 1 \pmod{4}$. So $p \equiv 1, 5 \pmod{8}$.

If $p \equiv 5 \pmod{8}$, then $5u^2 \equiv 1 \pmod{8}$. Hence $u^2 \equiv 5 \pmod{8}$, which is a contradiction. Consequently $p \equiv 1 \pmod{8}$. \square

Proposition 3.69. *If (b_6) has an integer solution, then $p, q \equiv 1 \pmod{8}$.*

Proof. If (b_6) has an integer solution, then $N^2 = pq(m^4 + 16e^4)$, $\gcd(m, pq) = 1$. There is an integer u that $pqu^2 = m^4 + 16e^4$.

From $m^4 \equiv -16e^4 \pmod{p}$, we have $(2em^*)^4 \equiv -1 \pmod{p}$. Consequently $p \equiv 1 \pmod{8}$.

From $m^4 \equiv -16e^4 \pmod{q}$, we have $(2em^*)^4 \equiv -1 \pmod{q}$. Consequently $q \equiv 1 \pmod{8}$. \square

Corollary 3.70. *The above results are summarized in the followings:*

- (1) $2 \in \text{Im}\alpha$ if and only if (a_1) has an integer solution. In this case, $p, q \equiv 1, 3, 7 \pmod{8}$.
- (2) $p \in \text{Im}\alpha$ if and only if (a_2) has an integer solution. In this case, $(\frac{\pm p}{q}) = +1 = (\frac{\pm 2q}{p})$.
- (3) $q \in \text{Im}\alpha$ if and only if (a_3) has an integer solution. In this case, $(\frac{\pm q}{p}) = +1 = (\frac{\pm 2p}{q})$.
- (4) $2p \in \text{Im}\alpha$ if and only if (a_4) has an integer solution. In this case, $(\frac{q}{p}) = +1 = (\frac{\pm 2p}{q})$.
- (5) $2q \in \text{Im}\alpha$ if and only if (a_5) has an integer solution. In this case, $(\frac{p}{q}) = +1 = (\frac{\pm 2q}{p})$.
- (6) $pq \in \text{Im}\alpha$ if and only if (a_6) has an integer solution. In this case, $p, q \equiv 1, 3, 7 \pmod{8}$.
- (7) $2pq \in \text{Im}\alpha$ if and only if (a_7) has an integer solution.
- (8) $p \in \text{Im}\bar{\alpha}$ if and only if (b_2) has an integer solution. In this case,

- $p \equiv 1 \pmod{8}, \left(\frac{p}{q}\right) = +1.$
 (9) $q \in Im\bar{\alpha}$ if and only if (b_3) has an integer solution. In this case,
 $q \equiv 1 \pmod{8}, \left(\frac{q}{p}\right) = +1.$
 (10) $pq \in Im\bar{\alpha}$ if and only if (b_6) has an integer solution. In this case,
 $p, q \equiv 1 \pmod{8}.$
 (11) $(b_1), (b_4), (b_5)$ and (b_7) does not have any integer solution.
 (12) If $p, q \equiv 5 \pmod{8}$ then $(a_2), (a_3), (a_4)$ and (a_5) does not have any integer solution.

Corollary 3.71. *By the previous corollary, we have:*

- (1) Let $p \equiv 1, q \equiv 5 \pmod{8}$ and $\left(\frac{p}{q}\right) = -1.$
 $(b_i), 1 \leq i \leq 7,$ does not have any integer solution. Hence $Im\bar{\alpha} = \{1\}.$
 By the quadratic reciprocity, we have $\left(\frac{q}{p}\right) = -1.$
 $\left(\frac{-p}{q}\right) = \left(\frac{p}{q}\right) = -1$ and $\left(\frac{-q}{p}\right) = \left(\frac{q}{p}\right) = -1.$
 It is possible for (a_7) to have integer solutions. So $Im\alpha \subseteq \{\pm 1, \pm 2pq\}.$
 As (2.1), implies $|Im\alpha| \geq 4.$ Consequently $Im\alpha = \{\pm 1, \pm 2pq\}.$
 Hence $r = 0,$ i.e., $2pq$ is not a congruent number.
- (2) Let $p \equiv 1, q \equiv 3, 7 \pmod{8}$ and $\left(\frac{p}{q}\right) = -1.$
 $(b_i), 1 \leq i \leq 7,$ does not have any integer solutions. Hence $Im\bar{\alpha} = \{1\}.$
 By the quadratic reciprocity, we have $\left(\frac{q}{p}\right) = -1.$
 $\left(\frac{-q}{p}\right) = \left(\frac{q}{p}\right) = -1$ and $\left(\frac{\pm 2q}{p}\right) = \left(\frac{\pm 2}{p}\right) \cdot \left(\frac{q}{p}\right) = -1.$
 It is possible for $(a_1), (a_6)$ and (a_7) to have integer solutions. So
 $Im\alpha \subseteq \{\pm 1, \pm 2, \pm pq, \pm 2pq\}.$
 Since $2pq$ is a congruent number, (see[4]), then $r \geq 1.$
 As (2.1), implies $Im\alpha = \{\pm 1, \pm 2, \pm pq, \pm 2pq\}.$ Hence $r = 1.$
- (3) Let $p \equiv 5 \pmod{8}$ and $q \equiv 3, 7 \pmod{8}.$
 $(b_i), 1 \leq i \leq 7,$ does not have any integer solution. Hence $Im\bar{\alpha} = \{1\}.$
 Since $2pq$ is a congruent number, (see[4]), then $r \geq 1.$
 It is possible for $(a_2), (a_3), (a_4), (a_5)$ and (a_7) to have integer solutions. So $Im\alpha \subseteq \{\pm 1, \pm p, \pm 2q, \pm 2pq\}$ or $\{\pm 1, \pm q, \pm 2p, \pm 2pq\}.$
 As (2.1), implies $Im\alpha = \{\pm 1, \pm p, \pm 2q, \pm 2pq\}$ or $\{\pm 1, \pm q, \pm 2p, \pm 2pq\}.$
 Hence $r = 1.$
- (4) Let $p, q \equiv 5 \pmod{8}.$

$(b_i), 1 \leq i \leq 7$, does not have any integer solution. Hence $Im\bar{\alpha} = \{1\}$.

It is possible for (a_7) to have integer solution. So $Im\alpha \subseteq \{\pm 1, \pm 2pq\}$.

As (2.1), implies $Im\alpha = \{\pm 1, \pm 2pq\}$.

Hence $r = 0$, i.e., $2pq$ is not a congruent number.

REFERENCES

- [1] B. J. Birch, Diophantine analysis and modular functions, International Colloquium on Algebraic Geometry, Tara Institute Studies in Mathematics 4, 3542 (1968).
- [2] H. Cohen, Number Theory. Vol. I: Tools and Diophantine Equations, Graduate Texts in Mathematics, 239 (Springer, New York, 2007).
- [3] K. Heegner, Diophantische analysis und modulfunktionen. Math. Z. 56, 227-253 (1952).
- [4] P. Monsky, Mock Heegner Points and Congruent Numbers, Math. Z. 204, 45-68 (1990) Mathematische Zeitschrift, 9 Springer-Verlag 1990.
- [5] T. Nagell, Lanalyse indetermineede degre superieur, Gauthier-Villars, Paris, (1929), 39, 16-17.
- [6] A. Silverman, Open questions in Arithmetic Geometry (Park, City ut, 1999), IAS/Par Mathamatics Series q, AMS, Providence, RI (2001), 85-142.
- [7] N. M. Stephens, Congruence properties of congruent numbers. Bull. Lond. Math. Soc. 7, 182-184 (1975)
- [8] J. B. Tunnell, A classical diophantine problem and modular forms. Invent. Math. 72, 323-334 (1983).
- [9] L. c. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman-Hall, 2008,
- [10] A. Adler, J. E. Coury, The Theory of Numbers : a Text and Source Book of Problems, Jones and Bartlett Publishers, 1995.

FARZALI IZADI DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, URMIA UNIVERSITY, URMIA 165-57153, IRAN

E-mail address: f.izadi@urmia.ac.ir

H. R. ABDOLMALEKI, DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, AZARBAIJAN SHAHID MADANI UNIVERSITY,, TABRIZ 53751-71379, IRAN

E-mail address: Hamid.Abdolmalki@gmail.com